INSO
18224-4

1st. Edition

2013

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندراد ایران
Iranian National Standardization Organization

استاندارد ملی ایران

۱۸۲۲۴-۴

چاپ اول

۱۳۹۱

فناوری‌اطلاعات – اتصال متقابل سامانه‌های باز– امنیت لایه‌های بالایی عام: ویژگی قاعده نحوی انتقال حفاظت

Information Technology-Open System Interconnection-Generic Upper Layers security: Protecting transfer syntax specification

ICS:35.100.01

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2 - International Electrotechnical Commission
3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فناوری‌اطلاعات – اتصال متقابل سامانه‌های باز– امنیت لایه‌های بالایی عام : ویژگی قاعده نحوی انتقال حفاظت»

رئیس:	**سمت و/ یا نمایندگی**
رضایی، رامین (لیسانس الکترونیک)	معاون طرح و توسعه مرکز تحقیقات صنایع انفورماتیک
دبیر:	
یحیایی، مهری (لیسانس کامپیوتر)	سرپرست آزمایشگاه فناوری اطلاعات مرکز تحقیقات صنایع انفورماتیک

اعضاء: (اسامی به ترتیب حروف الفبا)

افکار، علی (دکتری الکترونیک)	عضو هیات علمی دانشگاه علم و صنعت
ترابی، سعید (لیسانس مدیریت صنعتی)	مدیر فنی شرکت بازرسی کالای تجاری
حنیفه، فرشته (لیسانس اقتصاد)	کارشناس مرکز تحقیقات صنایع انفورماتیک
زندباف، عباس (لیسانس مخابرات)	کارشناس شرکت ارتباطات زیرساخت
فرج‌پور، مهیار (فوق‌لیسانس الکترونیک)	عضو هیات مدیره شرکت سیماوا
نادری، مجید (دکتری الکترونیک)	عضو هیات علمی دانشگاه علم و صنعت

فهرست مندرجات

پیش‌گفتار

استاندارد « فناوری اطلاعات: اتصال متقابل سامانه های باز- رویه های اجرایی برای عملکرد مراجع ثبت OSI قسمت ۲: رویه‌های ثبت برای انواع سند OSI » که پیش‌نویس آن در کمیسیون فنی مربوط، توسط مرکز تحقیقات صنایع انفورماتیک، تهیه شده و تدوین شده و در دویست و چهل و هشتمین اجلاسیه‌ی کمیته‌ی ملی استاندارد رایانه و فرآوری داده‌ها مورخ ۹۱/۱۱/۱۴ مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات سازمان ملی استاندارد ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه‌ی صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدیدنظر خواهد شد و هر پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، در هنگام تجدیدنظر در کمیسیون فنی مربوط، مورد توجه قرار خواهد گرفت. بنابراین، همواره از آخرین تجدیدنظر آنها استفاده خواهد شد.

منبع و ماخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته است به شرح زیر است:

ISO/IEC 11586-4: 1996 Information Technology-Open System Interconnection-Generic upper Layers security: Protecting transfer syntax specification

مقدمه

این استاندارد خدمت‌های فناوری‌اطلاعات – اتصال متقابل سامانه‌های باز– امنیت لایه‌های بالایی عام: ویژگی قواعد نحوی انتقال حفاظت‌کننده هدف و دامنه کاربرد که یک مجموعه امکانات را برای کمک به ساختن پروتکل‌های لایه‌های بالایی را که از آماده‌سازی خدمت‌های امنیت پشتیبانی می‌کند فراهم می‌آورد.

این قسمت‌ها به شرح زیر هستند:

قسمت ۱- مرور کلی، مدل و قواعد نحوی‌گذاری

قسمت ۲- تعریف خدمت عنصر خدمت تبادل امنیت

قسمت ۳- مشخصه پروتکل عنصر خدمت تبادل امنیت

قسمت ۴- مشخصه قواعد نحویی انتقال حفاظت‌کننده

قسمت ۵- پیش‌برگ PICS خدمت عنصر خدمت تبادل امنیت

قسمت ۶- پیش‌برگ PICS قواعد نحوی انتقال حفاظت‌کننده

این استاندارد ملی قسمت ۳ از این مجموعه را تشکیل می‌دهد.

فناوری‌اطلاعات – اتصال متقابل سامانه‌های باز– امنیت لایه‌های بالایی عام : ویژگی قواعد نحوی انتقال حفاظت‌کننده هدف و دامنه کاربرد

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد از مجموعه استانداردها، تعیین و فراهم نمودن یک دسته امکانات عام برای کمک به خدمات امنیتی در کاربردهای اتصال متقابل سامانه‌های باز (OSI)[1] می‌باشد. این امکانات شامل موارد زیر هستند:

الف) یک مجموعه ابزار قواعد نحوی‌گذاری به منظور پشتیبانی ویژگی الزامات حفاظتی فیلد انتخابی در یک ویژگی انتزاعی قواعد نحوی و پشتیبانی از مشخصات تبادلات امنیتی و دگرگونی‌های امنیتی.

ب) تعریف یک خدمت، ویژگی پروتکل و پیش‌برگ PICS برای یک عنصر-خدمت-کاربرد، به منظور پشتیبانی از فراهم‌کردن خدمات امنیتی درون لایه کاربردی OSI.

پ) یک مشخصه و پیش‌برگ پروتکل اجرا بیانیه انطباق (PICS)[2] برای یک مجموعه قواعد نحوی انتقال امنیتی، وابسته به پشتیبانی لایه بازنمود برای خدمت‌های امنیتی در این لایه کاربردی.

۱-۲ این استاندارد قواعد نحوی انتقال حفاظت‌کننده وابسته به پشتیبانی لایه بازنمود را برای خدمات امنیتی در لایه کاربردی تعریف می‌کند.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن‌ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی محسوب می‌شود.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد ملی الزامی است.[3]

توصیه‌نامه و استانداردهای بین‌المللی همسان

2-1 ITU-T Recommendation X.200 (1994) | ISO/IEC 7498:1994, Information technology – Open Systems Interconnection –Basic Reference Model: The Basic Model.

2-2 ITU-T Recommendation X.216(1994) | ISO/IEC 8822:1994, Information technology-Open Systems Interconnection – Presentation service definition.

1-Open System Interconnection

2-Protocol Implementation Conformance Statement

2-3 ITU-T Recommendation X.226(1994) | ISO/IEC 8823-1:1994, Information technology- Open Systems Interconnection – Connection-oriented presentation protocol: Protocol specification.

2-4 ITU-T Recommendation X.680(1994) | ISO/IEC 8824-1:1995, Information technology- Abstract Syntax Notation One(ASN.1): Specification of basic notation.

2-5 ITU-T Recommendation X.681(1994) | ISO/IEC 8824-2:1995, Information technology- Abstract Syntax Notation One(ASN.1): Information object specification.

2-6 ITU-T Recommendation X.682(1994) | ISO/IEC 8824-3:1995, Information technology- Abstract Syntax Notation One(ASN.1): Constraint specification.

2-7 ITU-T Recommendation X.683(1994) | ISO/IEC 8824-4:1995, Information technology- Abstract Syntax Notation One(ASN.1): Parameterization of ASN.1 specifications.

2-8 ITU-T Recommendation X.690(1994) | ISO/IEC 8825-1:1995, Information technology- ASN.1 encoding rules: Specification of Basic Encoding Rules(BER), Canonical Encoding Rules(CER) and Distinguished Encoding Rules(DER).

2-9 ITU-T Recommendation X.803(1994) | ISO/IEC 10745:1995, Information technology- Open System Interconnection-Upper layers security model.

2-10 ITU-T Recommendation X.830(1995) | ISO/IEC 11586-1:1996, Information technology- Open Systems Interconnection-Generic upper layers security: Overview, models and notation.

۳ اصطلاحات و تعاریف

۳-۱ این استاندارد از عبارات زیر که در ITU-T Rec. X.200|ISO/IEC 7498-1 تعریف شده‌اند استفاده می‌کند:

- قواعد نحوی انتقال

۳-۲ این استاندارد از عبارات زیر که در ITU-T Rec. X.216|ISO/IEC 8822 تعریف شده‌اند استفاده می‌کند:

- قواعد نحوی انتزاعی
- زمینه بازنمود
- مقدار داده بازنمود

۳-۳ این استاندارد از عبارات زیر که در ITU-T Rec. X.803|ISO/IEC 10745 تعریف شده‌اند استفاده می‌کند:

- وابستگی امنیتی
- تبدیل امنیتی

۳-۴ این استاندارد از عبارات زیر که در ITU-T Rec. X.830|ISO/IEC 11586-1 تعریف شده‌اند استفاده می‌کند:

- وابستگی امنیتی کران-زمینه-بازنمود[1] محدود به زمینه

1-Presentation-context-bound

- وابستگی امنیتی کران-مورد-تکی[1] محدود به تک مورد
- وابستگی امنیتی تاسیس‌شده در خارج
- مقررات کدگذاری اولیه
- زمینه بازنمود حفاظت‌کننده
- قواعد نحوی انتقال حفاظت‌کننده

۴ کوته‌نوشت‌ها

GULS	Generic Upper Layers Security	امنیت لایه‌های بالایی عام
OSI	Open system interconnection	اتصال‌متقابل سامانه‌های باز
PDU	Protocol-data-unit	واحد-داده-پروتکل
PDV	Presentation data value	مقدار داده بازنمود
PICS	Protocol implementation conformance statement	بیانیه انطباق پیاده‌سازی پروتکل

۵ مرور کلی

مفهوم یک مجموعه قواعد نحوی انتقال حفاظت‌کننده برای اولین بار در ITU-T Rec. X.830 | ISO/IEC 11586-1 ارائه شد. این مشخصه استاندارد، یک مجموعه قواعد نحوی انتقال حفاظت‌کننده عام را تعریف می‌کند. این مشخصه می‌تواند در رابطه با تعاریف تبدیل امنیتی خاص برای تولید یک مجموعه قواعد نحوی انتقالی حفاظت‌کننده، مناسب برآورده‌کردن الزامات حفاظت‌کننده کاربردهای خاص استفاده شود.

یادآوری- قواعد نحوی عام انتقالی حفاظت‌کننده ممکن است همچنین در تدارک فشرده‌سازی داده‌ها برای اهداف غیرمرتبط با امنیت نیز مورد استفاده قرار گیرد، اگرچه چنین استفاده‌ای خارج از حوزه این استاندارد است.

قواعد نحوی عام انتقال حفاظت‌کننده بر اساس مدل تبدیل امنیتی تعریف‌شده در ITU-T Rec. X.830 | ISO/IEC 11586-1 می‌باشد. هدف قواعد نحوی انتقال حفاظت‌کننده، فراهم‌کردن یک وسیله استاندارد برای ارائه موارد اطلاعاتی زیر به منظور اهداف انتقال و می‌باشد:

- مورد تبدیل‌شده‌ای که حاصل از استفاده فرایند کدگذاری یک تبدیل امنیت، به بازنمود یک مورد حفاظت‌نشده است که باید حفاظت شود.

1-Single-item-bound

- پارامترهای پویا و ایستای حفاظت‌شده‌ی یک تبدیل امنیتی، که حفاظت را از طریق پردازش‌شدن در فرایند کدگذاری یک تبدیل امنیتی (همراه با بازنمود مورد حفاظت‌نشده) بدست آورده‌اند.
- پارامترهای پویا و ایستا حفاظت‌نشده یک تبدیل امنیتی
- در اولین PDV زمینه بازنمود حفاظت‌شده، یا یک PDV حفاظت‌شده فرستاده‌شده به خارج از یک زمینه بازنمود، هر یک از موارد زیر:

الف) در مورد یک پیوستگی امنیتی نمایش محدود به زمینه یا محدود به تک موردی، یک شناسه تبدیل امنیت

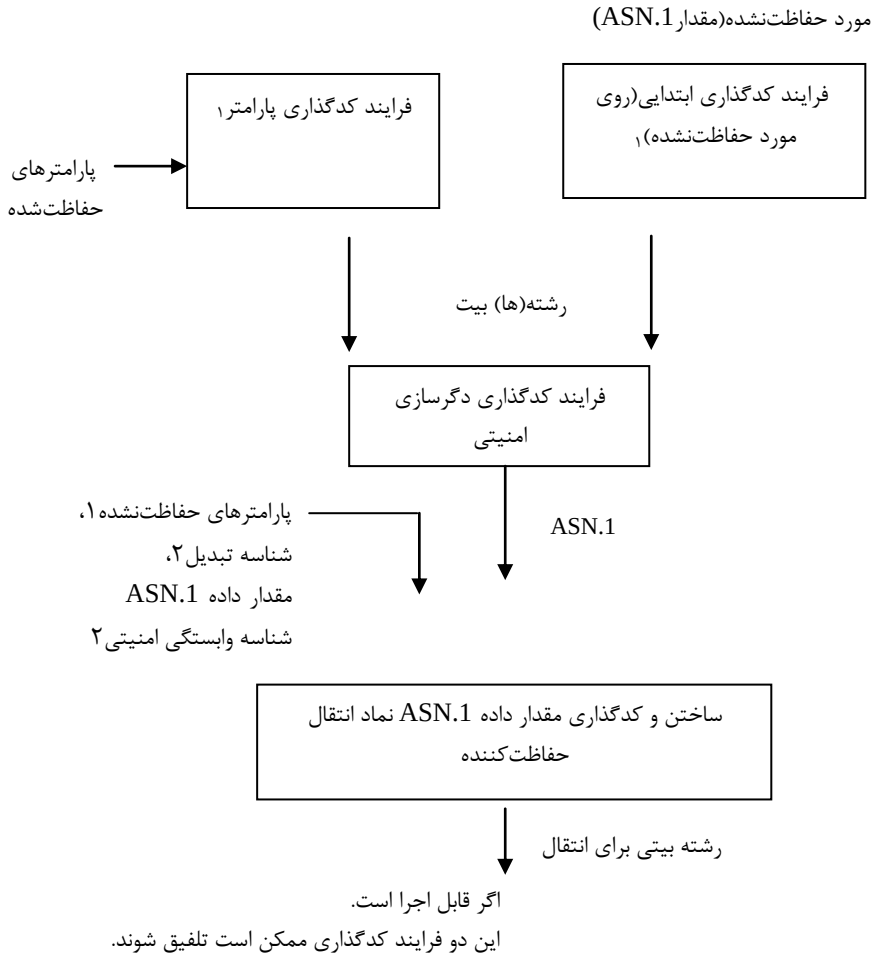
ب) در مورد یک پیوستگی امنیتی تاسیس شده در خارج، یک شناسه آن پیوستگی امنیتی

استفاده از قواعد نحوی انتقال حفاظت‌کننده توسط پروتکل بازنمود مطرح شده، یا در ساختار یک ASN.1 خارجی یا یک PDV جاسازی‌شده اعلام شده‌است. قواعد نحوی انتقال حفاظت‌کننده می‌تواند برای هر قواعد نحوی انتزاعی، که ممکن است با استفاده از ASN.1 یا به طرق دیگر مشخص شود، به‌کار گرفته شود. شناسه‌های شیئ برای مطرح یا اعلام‌کردن قواعد نحوی انتقال حفاظت‌شده در بند ۹ مورد ملاحظه قرار گرفته‌اند.

قواعد نحوی انتقال حفاظت‌کننده، یک قواعد نحوی انتقال حساس به زمینه می‌باشد، بعبارت دیگر وضعیت در بین رمزگذاران و رمزگشاها حفظ می‌شود.

۵-۱ مدل قواعد نحوی انتقال حفاظت‌کننده

شکل۱ عملیات مرتبط با قواعد نحوی انتقال حفاظت‌کننده را در یک سامانه کدگذاری، با جزئیات بهتری نسبت به ITU-T Rec. X.830 | ISO/IEC 11586-1 نمایش می‌دهد.(عملیات متناظر در یک سامانه رمزگشایی به طور طبیعی به دنبال می‌آید)



شکل۱- ساختن قواعد نحوی انتقال حفاظت‌کننده در سامانه کدگذاری

۵-۲ مقررات کدگذاری اولیه

مقررات کدگذاری اولیه (در سامانه کدگذاری) و فرایند رمزگشایی متناظر (در سامانه رمزگشایی) بین قواعد نحوی انتزاعی و قواعد نحوی حفاظت‌نشده نگاشت می‌کند. مقررات به‌کار برده‌شده در این فرایند به عنوان مقررات کدگذاری اولیه شناخته می‌شوند.

یادآوری- برای یک قواعد نحوی انتزاعی (ASN.1)[1] پایه، این نگاشت معمولا یک مجموعه جایگزین از مقررات کدگذاری ASN.1 به‌کار می‌گیرد.

1-Abstract Syntax Notation.1

قوانین کدگذاری تک مقداره(به عنوان مثال مقررات کدگذاری متعارف ASN.1 یا مقررات کدگذاری متمایز) بهتر است زمانی‌که تبدیل یک تابع از داده‌هاست که همچنین ممکن است جداگانه فرستاده‌شود، مخصوصا زمانی به‌کار برده‌شوند که از طریق یک سامانه رله استفاده می‌شود.

مقررات کدگذاری اولیه برای استفاده در یک قواعد نحوی انتقال حفاظت‌کننده به طور زیر مقرر شده‌است:

الف) اگر تبدیل امنیتی در حال استفاده از رساندن شناسه یک مجموعه مقررات کدگذاری خاص را به عنوان یک پارامتر ایستا (حفاظت‌شده یا حفاظت‌نشده) فراهم‌می‌آورد و اگر این پارامتر در فیلد اولین PDV قابل‌اجرا حاضر باشد، آن‌گاه این مقررات کدگذاری استفاده می‌شوند، در غیر این صورت:

ب) مقررات کدگذاری نشان داده‌شده توسط "مقررات کدگذاری اولیه" در زمینه تعاریف تبدیل امنیتی، استفاده می‌شوند.

۵-۳ تبدیل امنیتی

تبدیل امنیتی که باید به‌کار برده شود، توسط یکی از دو روش زیر اتخاذ می‌شود:

الف) زمانی‌که انتقال PDV به وابستگی امنیتی کران- زمینه- بازنمود یا بسته به - محصول- تک مرتبط می‌شود، شناسه تبدیل امنیتی در ساختار قواعد نحوی انتقال به همراه اولین PDV در آن پیوستگی امنیت منتقل می‌شود.

ب) زمانی‌که انتقال PDV به یک پیوستگی امنیت تاسیس‌شده خارجی مرتبط می‌شود، شناسه تبدیل امنیت یک صفت برای آن پیوستگی امنیت می‌شود.

مقررات تبدیل حاکی از چگونگی نگاشت یک آرایه بیت و یک مجموعه از مقادیر پارامترهای حفاظت‌شده به یک مقدار ASN.1 برای اهداف انتقال است.

۵-۴ ساختار قواعد نحوی

یک مجموعه قواعد نحوی انتقال حفاظت‌کنندهِ ساختار داده‌ِهای استفاده‌شده برای رساندنِ خروجی فرایندِ کدگذاری یک تبدیل امنیتی را به علاوه پارامترهای حفاظت‌نشده و شناسه‌های تبدیل امنیتی یا وابستگی امنیتی(اگر قابل اجرا است) تعریف می‌کند. ساختار داده‌های انتقال‌یافته، نوع متفاوت دیگری برای هر یک از حالات دارد:

الف) اولین PDV یک متن بازنمود حفاظت‌کننده در یک پیوستگی امنیتی بسته به زمینه-بازنمود، یا یک PDV در یک پوابستگی امنیتی بسته به محصول-تک

ب) اولین PDV یک متن بازنمود حفاظت‌کننده، یا یک PDV حفاظت‌شده فرستاده‌شده به خارج از یک زمینه بازنمود، در مورد وابستگی امنیتی تاسیس‌شده خارجی،

پ) PDV بعدی در یک زمینه بازنمود حفاظت‌کننده

۶ ساختارهای داده‌ها برای قواعد نحوی انتقال حفاظت‌کننده

ساختار داده استفاده‌شده توسط یک قواعد نحوی انتقال حفاظت‌کننده، توسط نوع ساختار قواعد نحوی ASN.1 در مدول ASN.1 زیر تعریف شده است. نوع ساختار قواعد نحوی با یک مجموعه شی ValidSTها

که مجموعه‌ای از اشیاء تبدیل امنیتی است پارامتری شده است. زمانی‌که یک مقدار برای ValidSTها فراهم‌می‌شود، به همراه مشخصات تبدیل امنیتی متناظر، نوع ساختار قواعد نحوی مشخصات کامل قواعد نحوی برای یک قواعد نحوی انتقال حفاظت‌کننده خاص می‌شود .

```
GenericProtectingTransferSyntax{joint-iso-ccitt genericULS(20)
            Modules (1) genericProtectingTransferSyntax (7)}
DEFINITIONS AUTOMATIC TAGS::=
BEGIN

EXPORTS
          SyntaxStructure {};
IMPORTS
          Notation
                FROM Object Identifiers {joint-iso-ccitt
                genericULS(20) modules (1) object Identifiers(0) }
          SECURITY-TRANSFORMATION, External SAID
                FROM Notation notation;
Syntax Structure{SECURITY-TRANSFORMATION: validSTs}::= CHOICE
{
                First Pdv Explicit          First Pdv Explicit {{ValidSTs}},
                --To be used on the first PDV of a protecting presentation
                --context, or a protected PDV sent outside a presentation
                --context, in the case of a presentation-context-bound or
                --single-item-bound security association
                First Pdv External        First Pdv External {{ValidSTs}},
                --To be used on the first PDV of a protecting presentation
                --context, or a protected PDV sent outside a presentation
                --context, in the case of an externally established
                -- security association
                subsequentPdv           SubsequentPdv {{ValidSTs}}
                --To be used on a subsequent Pdv in a protecting
                --presentation context.
}
First Pdv Explicit {SECURITY-TRANSFORMATION: ValidSTs}::=SEQUENCE
{
                Transformation Id SECURITY-TRANSFORMATION.&sT-Identifier
                      ({ValidSTs}),
                staticUnprotParm
                      SECURITY-TRANSFORMATION. & Static Unprotected Parm
                                  ({ValidSTs}{@transformation Id})
                                  OPTIONAL,
                dynamicUnprotParm
                      SECURITY-TRANSFORMATION.&DynamicUnprotectedParm
                                  ({ValidSTs}{@transformationId})
                                  OPTIONAL,
```

```
                xformedData SECURITY-TRANSFORMATION.&XformedDataType
                                ({ValidSTs}{@transformationId})
}

FirstPdvExternal  {SECURITY-TRANSFORMATION: ValidSTs}::=SEQUENCE
{
                External SAID       External SAID
                Dynamic Unprot Parm
                        SECURITY-TRANSFORMATION .& Dynamic Unprotected Parm
                                ({ValidSTs} OPTIONAL,
                                --Actual member of ValidSTs is as implied
                                --by external SAID
                Xformed Data SECURITY-TRANSFORMATION.& X formed Data Type
                                ({ValidSTs}
                                --Actual member of ValidSTs is as implied
                                --by externalSAID
}
subsequentPdv { SECURITY-TRANSFORMATION: ValidSTs}::=SEQUENCE
{
                dynamicUnprotParm
                        SECURITY-TRANSFORMATION.&DynamicUnprotectedParm
                                ({ValidSTs} OPTIONAL,
                X formed Data SECURITY-TRANSFORMATION. & X formed Data Type
                                ({ValidSTs}
                                --Actual member of ValidSTs is as implied
                                --by presentation context
}END
```

۷ تلفیق در پروتکل اصلی

زمانی‌که به یک بازنمود PDU مستقیما انتقال داده می‌شود (همان‌طور که در ITU-T Rec. X.226|ISO/IEC 8823-1 مشخص شده‌است) یا زمانی‌که در یک ساختار PDV ASN.1 جاسازی شده یا PDV خارجی، جاسازی شده‌است(همان‌طور که در ITU-T Rec. X.680|ISO/IEC 8824-1 مشخص شده‌است)، مقدار مناسب برای نوع ساختار قواعد نحوی، با استفاده از مقررات کدگذاری اشاره توسط شناسه شیئ قواعد نحوی انتقال، اگر وجود داشته‌باشد(به بند ۹ مراجعه‌شود)، یا به طور پیش‌فرض با استفاده از مقررات کدگذاری پایه ASN.1، کدگذاری می‌شود.

زمانی‌که به همراه گزینه مستقیم قواعد نحوی‌گذاری حفاظت‌شده یا حفاظت‌شده-Q مندرج در ITU-T Rec. X.830 | ISO/IEC 11586-1 استفاده می‌شود، ASN.1 نوع ساختار قواعد نحوی در ASN.1 برای پروتکل احاطه‌کننده وارد می‌شود و لذا با استفاده از مقررات ویژگی شده برای آن پروتکل کدگذاری می‌شود.

۸ رویه‌های اجرایی همزمان کردن

تمامی اطلاعات وضعیت باید زمانی‌که در مطابقت با مشخصات خدمت دیوره زمانی، یک نقطه همزمانی برقرار می‌شود، نگهداری شوند. اطلاعات وضعیت باید در هنگام وقوع یک همزمان کردن مجدد باز گردانده شوند.

یادآوری ۱- این استاندارد "وضعیت بازگردانی" را در همزمان کردن مجدد، را مشخص می‌کند. عملیات معادل بدون بازگردانی متن بازنمود در این استاندارد ارائه نشده‌است.

یادآوری۲- همزمان کردن مجدد به یک نقطه همگام فرعی ممکن است منتج به این شود که فرستادن هستار، از باب اینکه با دریافت موجودیت دریافت‌کننده تمامی تغییرات پارامترهای پویای اخیر را دریافت و اعمال شده است، اطمینان نباشد..

۹ انتصاب شناسه شیء

شناسه شیئ زیر به قواعد نحوی انتقال حفاظت‌کننده در این استاندارد ویژگی گردیده، انتصاب داده‌شده‌است:
{joint-iso-itu-t genericULS (20) generalTransferSyntax (2)}
استفاده از این شناسه شیئ لازم نمی‌دارد که یک مجموعه خاص مقررات کدگذاری برای کدگذاری مقدار ASN.1 ساختار قواعد نحوی استفاده شود، اما مقررات کدگذاری پایه ASN.1 به‌طور پیش‌فرض استفاده می‌شوند:
شناسه‌های شیئ بیشتری به قواعد نحوی انتقال حفاظت‌کننده تعریف‌شده در این استاندارد در زمانی‌که یک مجموعه مقررات کدگذاری خاص باید برای کدگذاری ساختار قواعد نحوی مقدار ASN.1 استفاده‌شوند، انتصاب داده شده‌اند. هر یک از مشخصات مقررات کدگذاری ASN.1 استاندارد(برای مثال آن‌هایی که در ITU-T Rec. X.690 | ISO/IEC 8825-1 تعریف شده‌اند) ممکن است مشروط باشد. قرارداد زیر به‌کار گرفته می‌شود. شناسه شیئ با پیشوند زیر شروع می‌شود:
{joint-iso-itu-t genericULS (20) specificTransferSyntax (3)……}
مقادیر باقی‌مانده همان مقادیری هستند که به دنبال پیشوند زیر آورده می‌شوند:
{joint-iso-itu-t asn1 (1)…}
که برای موارد مقررات کدگذاری ASN.1 معمولی.

۱۰ مطابقت

یک سامانه مدعی انطباق با این استاندارد، در زمان استفاده از قواعد نحوی انتقال حفاظت‌کننده آن‌طور که توسط شناسه شیئ ASN.1 برای مدول "قواعد نحوی انتقال حفاظت‌کننده عام" که در بند۶ ارائه شده، تعریف شده‌است، باید کاربردها ASN.1 قابل کاربرد و همه شرایط مربوطه را پشتیبانی‌کند.